L'analisi del rischio nell'ambito della gestione della sicurezza delle informazioni

Enrico Cavalli
CILEA, Segrate

Abstrac
L'analisi del rischio è un tassello fondamentale nella gestione della sicurezza delle informazioni. E' parte integrante della fase di pianificazione prevista dallo standard ISO 17799, ed è un'occasione importante per le aziende che vogliano affrontare con ampio respiro il problema della sicurezza dei propri dati.

Keywords: Telematica, Sicurezza, ISO 17799, Risk analysis, Risk assessment, Threat assessment, Analisi del rischio.

Introduzione

Nel numero precedente del Bollettino del CILEA [1] abbiamo introdotto la problematica della gestione della sicurezza in ambito informativo, come previsto dallo standard internazionale ISO 17799. Abbiamo mostrato che la necessità della sicurezza è strettamente legata al valore di un'informazione: tanto questo è più alto, tanto più saremo disposti o costretti a spendere per proteggerlo.

Abbiamo altresì affermato che la gestione della sicurezza è un fatto prettamente manageriale e non soltanto tecnologico come spesso si tende a considerarlo, senza però scendere nei dettagli di come si possa operare nella pratica. Vogliamo ora approfondire il punto centrale della questione, ovvero l'analisi del rischio quale strumento indispensabile nella pianificazione di un sistema di gestione della sicurezza.

Il ciclo di gestione della sicurezza

Gestire la sicurezza è innanzitutto un processo manageriale che si articola in un ciclo di quattro fasi: la progettazione, l'implementazione, il controllo e la revisione. Gli anglosassoni definiscono questo modello come PDCA: *Plan-Do-Check-Act*. La progettazione di un sistema di gestione della sicurezza – o *ISMS, Information Security Management System* - è la fase sulla quale ci concentreremo maggiormente in questo articolo. Progettazione significa innanzitutto stabilire delle policy, delle linee guida per la gestione del rischio. Si individuano degli obiettivi da perseguire e si strutturano i processi atti a controllare il rischio. Cosa esattamente sia il rischio lo definiremo solo in conclusione dell'articolo: intuitivamente possiamo dire che si tratta della possibilità che un'informazione o sistema informativo venga "intaccato" da un agente di minaccia, tramite una vulnerabilità del sistema stesso.

In questo articolo non tratteremo la fase operativa, il "Do" di PDCA, in quanto riteniamo che sia più sensato esaminarla caso per caso e alla luce di quanto verrebbe evidenziato dalla fase di pianificazione.

Sarebbe invece interessante parlare, e lo faremo in un articolo successivo, della fasi "*Check*"e "*Act*". In queste ultime due fasi di un processo di gestione della sicurezza, ci si concentra sulla misurazione e sul confronto delle performance del processo "gestione della sicurezza" rispetto a criteri stabiliti in fase progettuale. Il discorso è molto interessante e merita il dovuto approfondimento. Non nascondiamo il fatto che misurare le performance di un processo essenzialmente percepito in perdita debba essere oggetto di ulteriori studi. Cosa possiamo misurare? Si hanno solo costi o anche ricavi dal gestire la sicurezza? I ricavi sono solo mancate perdite? Dobbiamo affidarci al solo valore economico, oppure esistono altri indicatori di performance utilizzabili in questo caso?

La progettazione

La prima difficoltà che si incontra progettando un sistema di gestione della sicurezza, è stabilire in maniera precisa l'ambito dello stesso e i risultati che si vogliono ottenere.
Chi siamo? Di quali risorse informative disponiamo? Sono queste le prime due domande cui è opportuno rispondere, perché da queste scaturisce naturalmente un diverso approccio alla problematica della sicurezza. Una banca ragiona diversamente da un'università. Un ospedale percepisce la sicurezza in maniera diversa rispetto ad un'azienda manifatturiera. Una piccola-media impresa sente la sicurezza diversamente da come la sente una grande multinazionale.
Dimensioni e tipologia di business sono due fattori che condizionano profondamente l'approccio alla sicurezza. A seconda della natura, un'azienda avrà un diverso atteggiamento e una diversa sensibilità per la sicurezza. E, naturalmente, saranno diversi i requisiti e le esigenze stesse di sicurezza.

La fase progettuale serve ad evidenziare questa sensibilità e a determinare i livelli di sicurezza richiesti dalle varie risorse informative presenti in azienda. Si tratta quindi di effettuare una sorta di inventario dei sistemi informativi, e di applicarvi un'analisi dei requisiti di confidenzialità, integrità e disponibilità: i tre parametri che definiscono la sicurezza, come vedremo meglio in seguito.

Questo inventario potrebbe anche essere, almeno inizialmente, un semplice elenco dei vari server, database e applicativi presenti in azienda. Naturalmente uno sterile elenco ci fornisce poche informazioni e non consente una progettazione efficace. Le risorse informative devono essere infatti calate nella realtà aziendale, per capirne le interconnessioni e la relativa importanza.

A questo scopo può risultare molto utile la mappatura per processi. Questa è uno strumento di analisi organizzativa e gestionale dell'azienda ormai molto diffuso e parte integrante di molti corsi accademici. Non possiamo affrontare il discorso in questa sede, ma diamo un semplice riferimento bibliografico [2] per chi volesse approfondire l'argomento. Semplificando agli estremi, mappare un'azienda per processi significa individuare i processi aziendali e i loro elementi chiave, ovvero le risorse umane e tecnologiche che vi partecipano. I processi sono quindi delle scatole chiuse, in cui un input, mischiato a determinati ingredienti, produce un output ben preciso. L'output di un processo è un cliente, interno oppure esterno all'azienda.

Calare le risorse informative in una mappatura per processi, da un lato ci aiuta quindi a contestualizzare le informazioni nell'azienda, dall'altro evidenzia la relativa criticità di ciascuna risorsa. Alcuni processi sono più importanti di altri, nel senso che contribuiscono in maniera più incisiva sul business complessivo dell'azienda. Un processo fa uso di risorse anche informative, quindi queste hanno importanza se messe in relazione con il business, o meglio con l'apporto di un processo al business complessivo dell'azienda.

Sovente, specie all'inizio, conviene definire accuratamente l'ambito di un ISMS, e quindi del risk-assessment. Meglio partire considerando l'azienda divisa in grandi macro-processi che fanno uso di risorse informative molto generali, per poi scendere a dettagli maggiori in analisi successive. Per fare un esempio concreto, che aiuti anche a capire meglio l'idea stessa di mappatura per processi, consideriamo un'astratta industria che produce macchine utensili. I macro-processi operativi sicuramente presenti in questa azienda sono la logistica in ingresso, la produzione (di lavorati e semi-lavorati), la vendita o commercializzazione dei prodotti, la logistica in uscita. Come si nota anche dall'ordine con cui sono esposti, ogni processo produce un output che diventa l'input del processo seguente. Quelli descritti sono processi verticali, operativi. Trasversalmente a questi si hanno dei processi orizzontali, non propriamente operativi, ma comunque importanti in quanto funzionali ai precedenti. Tra questi vi sarà l'amministrazione, la gestione dei sistemi informativi, la ricerca e sviluppo di nuovi macchinari, la gestione delle risorse umane e così via. Gli economisti ritroveranno, in questa visione estremamente semplificata di azienda, la famosa catena del valore di Porter.

Solo l'esperienza può aiutare nell'aggiustare la granularità con cui conviene ragionare in termini di processi e risorse. Consideriamo ad esempio una risorsa informativa presente praticamente in ogni azienda: “i PC dei dipendenti”. Ha senso considerarli come una risorsa unica, oppure è necessario scendere nel dettaglio e considerare ogni PC come una risorsa a sé stante? In altre parole, è più sensato ragionare in termini di “postazioni di lavoro del personale” oppure considerare il “PC di Mario Rossi”, il “PC di Giovanni Bianchi” e così via?

Nella realtà converrà magari utilizzare una giusta via di mezzo: ad esempio i "PC dei dipendenti dell'amministrazione" potrebbero essere considerati una risorsa con requisiti di sicurezza diversi dai "PC dei ricercatori del laboratorio segreto".

Preparazione all'analisi delle minacce e del rischio

Dopo aver determinato quali risorse prendere in considerazione, ovvero dopo aver determinato l'ambito della nostra analisi del rischio, dobbiamo identificare un team di persone in grado di svolgere puntualmente tale analisi. Il team deve essere rappresentativo del sistema o risorsa presa in considerazione, e possibilmente deve essere multidisciplinare. Ad esempio se consideriamo un applicativo dedicato alla gestione contabile della nostra azienda, il team dovrà includere sia gli amministratori del sistema, sia un rappresentate degli utenti che effettivamente utilizzano l'applicativo.

Questo è fondamentale per riuscire ad ottenere una visione non di parte sul sistema informativo preso in considerazione. Come vedremo meglio nel seguito, soprattutto quando si considera la disponibilità di un dato sistema informativo, possono scatenarsi conflitti che è bene prevedere. E' consigliabile stabilire una procedura per dirimere punti di vista discordanti che possono emergere nelle valutazioni dei membri dei team.

Valutazione dei requisiti di sicurezza

Per valutare i requisiti di sicurezza si utilizzano in genere dei questionari che i team multidisciplinari sopra individuati dovranno compilare. Scopo di tali questionari è identificare i tre requisiti fondamentali per la sicurezza di qualsiasi informazione o sistema informativo: confidenzialità, integrità e disponibilità. Valutare per lo meno qualitativamente questi requisiti è importante per determinare l'impatto che deriverebbe dal venir meno anche di uno solo di questi. Segnaliamo che è possibile un tipo di analisi estremamente più accurato, che assegna un peso economico a ciascuna delle valutazioni: la complessità dell'analisi però aumenta notevolmente.

Valutare la confidenzialità significa stabilire quanto un'informazione sia sensibile alla divulgazione. Spesso occorre considerare la confidenzialità come una variabile dipendente dal tempo. Ad esempio alcuni dati di ricerca possono essere confidenziali mentre la ricerca è in corso, e non essere più tali una volta che i risultati vengano pubblicati. In altri casi i singoli dati non sono confidenziali di per sé, ma possono diventarlo in forma aggregata. Se ad esempio consideriamo gli approvvigionamenti di armamenti, i dati su una singola caserma possono avere un grado di confidenzialità minore rispetto all'aggregato di più basi militari.

Sarà opportuno preparare delle checklist per aiutare i compilatori dei questionari nella valutazione della confidenzialità. Ad esempio potrebbe essere utile rispondere alle seguenti domande:

- l'informazione trattata contiene dati personali? Riguarda dati ritenuti sensibili ai sensi della legge 657/96?
- quali conseguenze si avrebbero da una perdita di confidenzialità? Danni economici? Perdita di fiducia della nostra clientela?

Veniamo ora al requisito di integrità. Questo forse è il parametro più difficile da valutare, in quanto è definito come l'accuratezza e la completezza di un'informazione. I requisiti di integrità sono molto alti per esempio nel caso di transazioni bancarie, dove una perdita di integrità si traduce facilmente in perdite finanziarie. Le domande da porsi in questo caso sono:

- qual è l'impatto di dati non accurati?
- qual è l'impatto di dati non completi?

Probabilmente a nessuno di noi verrebbe mai in mente di dichiarare che dati non accurati o incompleti possano essere in qualche misura accettabili. Dopo tutto chi sarebbe disposto ad accettare dati inesatti? Allora perché mai occuparsi dell'integrità, se un dato deve sempre essere integro? L'esempio forse più immediato per capire che a volte conviene invece soffermarsi a soppesare attentamente i requisiti di integrità, è il seguente: un errore in una cartella clinica di un paziente, ad esempio un gruppo sanguigno errato, ha la stessa gravità rispetto ad un numero sbagliato in una rubrica telefonica? Quanto costa rintracciare il numero corretto? Quanto costa una trasfusione sbagliata?

Per finire consideriamo la disponibilità di una risorsa informativa. Un sistema è considerato disponibile se utilizzabile dagli utenti autorizzati. Da un lato i *downtime* non prevedibili di un sistema informativo sono un dato pressoché certo, in assenza di opportune misure di sicurezza quali la ridondanza delle componenti più suscettibili di guasto. Daltra parte è opportuno valutare fino a che punto i processi aziendali risentono

dell'indisponiblità di un sistema informativo. È assolutamente indispensabile stabilire i massimi livelli di downtime accettabili per l'azienda. Attenzione a quanto c'è scritto: accettabili per l'azienda, **non** accettabili per il singolo reparto o addirittura per il singolo impiegato. Spesso ciò significa dover mediare tra diversi gruppi di utenti: il direttore dell'amministrazione riterrà estremamente importante la disponibilità del programma di elaborazione delle fatture, ma in realtà per quanto tempo tale sistema può restare indisponibile senza che i processi amministrativi subiscano gravi rallentamenti?

Valutazione delle minacce

Stabiliti i requisiti di sicurezza, si passa a considerare quali agenti avversi potrebbero inficiarla: le minacce. Queste possono essere divise in due grandi categorie: le minacce che agiscono con un movente, e quelle che agiscono senza movente. Nella seconda classe rientrano tutti gli agenti casuali, quali incendi, inondazioni, sbalzi di tensione, guasti hardware e così via. Nella prima classe rientrano invece le azioni deliberate, ad esempio furti o danni volontariamente causati da personale interno piuttosto che da *hacker* esterni. Questa distinzione è importante quando considereremo in seguito la probabilità di una minaccia.

Se lo si ritiene opportuno, potrebbe essere utile considerare le minacce appartenenti a classi omogenee. Un possibile modello idoneo a raggruppare le minacce è il seguente:

- **divulgazione di dati classificati**: esempi di minacce sono intercettazioni, hacker, procedure di manutenzione non corrette;
- **interruzione di servizio**: ad esempio terremoti, incendi, inondazioni, mancanza di tensione elettrica;
- **modifica di dati**: errori nel data entry, hackers;
- **distruzione**: terremoti, incendi, inondazioni, sbalzi di tensione;
- **rimozione**: furto di dati, furto di sistemi.

Ovviamente questi sono solo esempi, e d'altra parte si tratta di un aspetto facoltativo dell'analisi delle minacce. Potrebbe essere utile come informazione aggiuntiva da riportare nei report conclusivi, a fini statistici.

Invece è sicuramente più utile avere a disposizione elenchi standard di minacce. In questo caso possiamo consigliare due fonti:

- l'elenco di minacce dell'*IT Baseline Protection Manual* del BSI tedesco [3];
- l'elenco delle misure di sicurezza dello standard ISO 17799: questo è da interpretare in maniera duale, ovvero ritenendo una minaccia la mancanza di uno dei controlli previsti dallo standard.

Ogni team dovrà avere accesso all'elenco scelto da chi progetta l'analisi del rischio, e dovrà trarne ispirazione, per così dire. Se tutti hanno a disposizione un elenco precostituito che consideri un'ampia casistica, potremo essere sicuri che l'analisi non trascurerà per lo meno le minacce che vengono solitamente considerate in letteratura.

Come già accennato, ogni minaccia ha una probabilità di verificarsi. Dobbiamo ora mappare ogni minaccia in tre classi di probabilità: bassa, media, alta. In taluni casi potrebbe essere sensato considerare una quarta classe, non applicabile, ad esempio per indicare che una minaccia non è nemmeno ritenuta rilevante. Si noti che l'aspetto probabilistico assume due connotazioni distinte se consideriamo un agente casuale quale un evento distruttivo naturale, piuttosto che un agente deliberato di minaccia quale può essere il furto di dati da parte di un hacker. Nel primo caso sarebbe opportuno avere a disposizione dati statistici interni alla propria organizzazione, oppure ci si può rifare a dati storici dell'area geografica nella quale si opera. Nel secondo caso occorre ragionare in termini diversi, considerando sia l'agente, sia il beneficio che tale agente otterrebbe nel perpetrare la minaccia, ad esempio un furto. Tanto più il beneficio per l'agente è alto, tanto maggiore sarà la motivazione che l'agente ne ricava e quindi, dal nostro punto di vista, tanto maggiore sarà la probabilità che la minaccia si verifichi.

Una minaccia, per quanto grave e per quanto sia ritenuta probabile, non ha senso se considerata disgiunta dall'impatto che questa potrebbe avere. Ecco perché è ora importante valutare l'impatto di una minaccia, considerata **in assenza di misure di sicurezza**. Nella fase successiva della nostra analisi valuteremo poi il rischio, considerando invece le misure di sicurezza esistenti o proponendone di nuove. L'impatto deve essere valutato mappando le conseguenze in una scala a tre valori: basso, medio e alto.

E' essenziale identificare degli scenari per mappare gli impatti su questa scala. Gli scenari che possiamo prendere in considerazione sono tanti: facciamo quindi alcuni esempi sottolineando

però che questa mappatura deve essere stabilita prima di iniziare l'analisi del rischio. Deve inoltre essere stabilita una volta per tutte, in maniera obiettiva ed omogenea per tutti i sistemi che stiamo prendendo in considerazione. Ecco allora alcuni possibili scenari di impatto:

- **danni alle persone**: una lieve ferita avrà impatto basso, la morte di una persona impatto alto;
- **perdita finanziaria**: basta stabilire delle soglie tramite le quali definire un impatto basso, medio oppure alto: ad esempio perdita<100.000€ uguale impatto medio, perdita > 100.000€ uguale impatto alto;
- **degrado nell'erogazione di un servizio**: per esempio si può adottare una scala temporale e ritenere basso l'impatto di un degrado di durata inferiore all'ora, medio da un'ora a 24 ore, alto se maggiore di un giorno;
- **conseguenze legali**: qui rientrano le violazioni di leggi, le violazioni di obblighi contrattuali, violazioni di copyright, etc.;
- **violazione della privacy**: potrebbe essere utile prevedere uno scenario ad hoc, anche se si può far rientrare la violazione della privacy nelle conseguenze legali;
- **divulgazione di informazioni confidenziali;**
- **danni all'ambiente**: per alcune aziende potrebbe essere uno scenario da tenere in considerazione, in quanto è una tematica cui l'opinione pubblica oggi presta molta attenzione;
- **relazioni con l'esterno.**

Se da un lato non è strettamente indispensabile prevedere uno scenario in cui far rientrare ogni possibile disastro (di alcune minacce si intuisce in maniera evidente il possibile impatto), d'altra parte avere dei riferimenti comuni e prestabiliti aiuterà ad ottenere un'analisi più precisa. Conviene quindi spendere un po' di tempo in fase progettuale per costruirsi degli scenari di impatto sufficientemente realistici e sufficientemente esaustivi, in maniera tale da non lasciare un'estrema libertà ai team di analisi.

Arrivati a questo punto è finalmente possibile determinare un livello di esposizione ad una data minaccia, utilizzando ad esempio lo schema riportato in Tabella 1.

		IMPATTO		
		Alto	Medio	Basso
PROBABILITA	Alta	9	8	5
	Media	7	6	3
	Bassa	4	2	1

Tabella1: La valutazione del grado di esposizione ad una minaccia. Si noti come venga dato maggiore peso all'impatto, piuttosto che alla probabilità.

Va da sé che i risultati fin qui ottenuti sono già piuttosto significativi, perché assegnare un livello di esposizione ad ogni minaccia su ogni risorsa, ci fornisce immediatamente un indicatore importante su cosa proteggere e sulle eventuali priorità di intervento.

Il concetto di rischio

Finalmente siamo pronti a valutare il rischio che, dopo tutto il lavoro fin qua svolto, non abbiamo in realtà definito puntualmente. La differenza sostanziale tra la valutazione delle minacce e la valutazione del rischio sta nel considerare le misure di sicurezza esistenti, che solo ora entrano in gioco. Si può definire il rischio come la possibilità che una minaccia si verifichi, o meglio come la possibilità che una vulnerabilità venga sfruttata e dia luogo all'attuazione di una minaccia.

L'analisi del rischio deve essere effettuata prendendo in considerazione le misure di sicurezza esistenti, e poi quelle che si ritiene necessario introdurre per diminuire un rischio troppo elevato. Valutare un rischio significa quindi mettere sui piatti della bilancia le minacce da una parte e i controlli, le misure di sicurezza dall'altra. Se le minacce "pesano" di più, potrebbe essere necessario introdurre nuove misure di sicurezza. Negli altri casi di equilibrio, o quando addirittura si ritiene che i controlli superino la gravità della minaccia, non è normalmente necessario intervenire proponendo nuove misure

di sicurezza. Non dimentichiamo però alcune considerazioni di natura criminologica che possiamo certamente applicare anche in questo caso:

- una minaccia ha una probabilità di verificarsi;
- ci può essere una possibile motivazione da prendere in considerazione;
- che valore ha la risorsa in considerazione, per l'azienda da un lato e per l'agente di minaccia dall'altro;
- quale sforzo è richiesto all'agente minaccioso per sfruttare una nostra vulnerabilità.

Tutto questo per dire che non basta affermare che una vulnerabilità esiste, e automaticamente questa verrà sfruttata. Normalmente devono sussistere altre condizioni al contorno sopra evidenziate.
Fatte queste debite premesse si può ricavare un livello di rischio. Ancora una volta si potrà decidere di mappare il rischio su una scala a tre valori, i soliti basso, medio e alto. Indipendentemente dalla scala adottata, potrebbe esistere una policy, stabilita dall'alta direzione, che dica che i rischi alti devono immediatamente essere presi in considerazione, mentre ad esempio i rischi ritenuti estremamente bassi possano essere accettati senza nemmeno richiedere l'approvazione della direzione. Qui si entra troppo nel dettaglio o nel caso concerto, ma ovviamente ci si può sbizzarrire nel trovare il criterio più adatto alle proprie esigenze.
In ogni caso se viene rilevato un rischio, possiamo agire sostanzialmente in quattro modi:

- accettare con cognizione di causa e obiettivamente (in conformità alla policy aziendale) il rischio;
- applicare appropriate misure di sicurezza per ridurre il rischio ad un livello più basso;
- evitare il rischio;
- trasferire il rischio a terzi (ad esempio ai fornitori, oppure stipulando polizze assicurative).

Se i primi due casi sono del tutto intuitivi, forse è bene spendere qualche parola per chiarire cosa si intende con evitare o trasferire un rischio. Consideriamo ad esempio un'azienda operante nella grande distribuzione, con vasti magazzini e un'imponente movimentazione logistica. Questa azienda potrebbe subire furti dei propri TIR, o nei propri magazzini. Una soluzione a questo problema potrebbe consistere nel trasferire il rischio ad un fornitore, affidando tutta la logistica a terze parti. Il rischio rimane, ma viene trasferito, senza utilizzare la classica formula di trasferimento: quella assicurativa.
I rischi possono anche essere evitati, ma in questo caso è più difficile fare esempi concreti. Alcune grandi multinazionali che operano anche nei generi alimentari, hanno un certo grado di rischio per il solo fatto di fare ricerca sugli OGM, Organismi Geneticamente Modificati. È risaputo che alcuni attivisti contrari a questo tipo di produzione organizzano a volte manifestazioni o atti di disturbo che possono arrecare danno alle aziende. Tutti ricorderanno il panettone avvelenato di Motta/Nestlé... Senza entrare nel merito della questione, alcune aziende alimentari evitano del tutto questo tipo di rischio semplicemente con politiche aziendali. In questa direzione si muovono per esempio la comunicazione e le scelte aziendali di varie aziende che puntano invece sulla genuinità dei propri prodotti.

Conclusioni

Il rischio, purtroppo, non sempre può essere evitato o ridotto. Gli incidenti di sicurezza capitano comunque, e il sistema di gestione della sicurezza non può prescindere dal definire anche le modalità di gestione degli incidenti. Ad esempio una migliore comunicazione tra azienda e consumatore, nel caso di Motta, avrebbe forse potuto evitare le ingenti perdite dell'azienda. Il ritiro di tutti i panettoni dal mercato, seguito da una campagna pubblicitaria per rassicurare il cliente, avrebbe sicuramente fatto una migliore impressione sul consumatore rispetto alla sostanziale inazione che all'epoca dei fatti l'azienda adottò come politica nelle relazioni esterne. Tra parentesi, il panettone avvelenato effettivamente rinvenuto fu proprio uno solo, ma le perdite per l'azienda furono ingenti. Alcuni vedono, come fattori che contribuirono a tali perdite, il fatto che Motta si affidò quasi esclusivamente alla (lenta) azione della magistratura.
Saper gestire gli incidenti quando questi inevitabilmente accadono, è quindi essenziale e parte integrante di un ISMS. Qualcuno si sta domandando cosa c'entrino gli attivisti di una qualsivoglia fazione con la gestione della sicurezza informatica? Una risposta la potete trovare su http://www.netsrike.it/, senza colpevolizzare né esaltare nessuno. Quel sito è la semplice constatazione che le classiche dinamiche sociali si stanno poco a poco riproponendo nel mondo dell'informazione digitale. Un manager della sicurezza informativa non può non tenerne conto.

Per concludere, segnaliamo che il risk-assessment può essere affidato ad aziende di consulenza, senza però prescindere da un forte coinvolgimento di risorse interne all'azienda. Il CILEA sta attualmente operando in questo settore presso alcune importanti strutture sanitarie. L'esperienza maturata in questo settore, per quanto specifica, può essere riproposta ad enti accademici e di ricerca, oltre che ad aziende private.

Bibliografia

[1] E. Cavalli, "*Sicurezza informatica: un'opportunità oppure l'ennesima incombenza da sopportare?",* Bollettino del CILEA, n. 85, Dicembre 2002

[2] Johansson, McHugh, Pendelbury, Wheeler, *Business Process Re-engineering*. Wiley, 1993.

[3] BSI, URL: http://www.bsi.de/gshb/english/menue.htm